UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

DANIELLE ROSENFELD and VINCENT GARCIA, on behalf of themselves and all others similarly situated,

Plaintiffs,

-against-

TARA LENICH; CITY OF NEW YORK; LU-SHAWN M. THOMPSON, AS ADMINISTRATOR OF ESTATE OF KENNETH P. THOMPSON; ERIC GONZALEZ; MARK FELDMAN; WILLIAM SCHAEFER; BRIAN DONOHUE; WILLIAM POWER; MICHAEL DOWLING; JOSEPH PIRAINO; and ROBERT KENAVAN,

Defendants.

CLASS ACTION COMPLAINT & JURY DEMAND

No. 18 Civ. ____

Plaintiffs Danielle Rosenfeld and Vincent Garcia ("Plaintiffs"), through their undersigned counsel, on behalf of themselves and all persons similarly situated, allege the following based on personal knowledge as to allegations regarding Plaintiffs and on information and belief as to other allegations:

PRELIMINARY STATEMENT

Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping.

Olmstead v. United States, 277 U.S. 438, 475–76 (1928) (Brandeis, *J.*, dissenting)

1. For eighteen months, King's County Supervisory Assistant District Attorney Tara Lenich ("Lenich") conducted an illegal wiretapping operation targeting two coworkers, Assistant

District Attorney Stephanie Rosenfeld and New York Police Department Detective First Grade Jarret Lemieux. She did so using her authority as Deputy Chief of Special Investigations of Violent Criminal Enterprises in the King's County District Attorney's Office ("KCDA" or "the Office") and as a supervisor of the KCDA's wire room operations. She did so using the equipment, facilities, and funds of the KCDA. And she did so in plain view of two District Attorneys and other supervisors within the KCDA, who allowed her to conduct a "confidential" investigation involving a round-the-clock wiretap on two cellular phones every hour of every day for well over a year, yielding hundreds of hours of recorded conversations, all stored on KCDA servers accessible to others within the Office.

2. Lenich's scheme would have been easily detected within the first month had her supervisors complied with their obligations under state and federal law to keep records of all KCDA wiretaps for the purpose of reporting statistics to the Administrative Office of United States Courts. But the Administrative Office Wiretap Reports for Calendar Years 2015 and 2016 indicate that "[n]o prosecutor's report" was received in those years—the two years during which Lenich carried out her scheme. Notably, the Administrative Office Wiretap Reports for 2014 and 2017—the years preceding and following the illegal wiretaps—reflect data presumably submitted by the KCDA.

3. This illegal wiretapping operation caused serious harm to Ms. Rosenfeld and Det. Lemieux, who have each filed federal lawsuits seeking to recover for their substantial injuries. But they are not its only victims.

4. Not one of the hundreds of individuals who spoke to, or exchanged text messages with, Ms. Rosenfeld or Det. Lemieux during the time their cellular phones were illegally tapped consented to their conversations being intercepted or recorded. Each of these individuals is the

victim of a serious invasion of privacy carried out by a high-ranking New York City official, acting in the course of her employment, on City time, using City equipment and facilities, and financed by City funds.

5. Federal law provides each of these victims with a statutory remedy. Under the Wiretap Act, each and every "person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation" of the Act, is entitled to relief, including actual or liquidated damages, punitive damages, and attorneys' fees. 18 U.S.C. § 2520.

6. Through this class-action lawsuit, Plaintiffs seek to recover statutory damages on behalf of themselves and all others similarly situated, whose communications were illegally intercepted during the course of Ms. Lenich's illegal wiretapping operation. The class consists of at least 700 individuals, each of whom is entitled to statutory liquidated damages of at least $10,000.

7. In addition, Plaintiffs seek punitive damages against the individual defendants in light of the reckless—and in the case of Lenich, intentional and malicious—violation of each victim's privacy rights during the course of the wiretapping operation.

PARTIES

8. Plaintiff Danielle Rosenfeld is a citizen and resident of the State of California. She is Stephanie Rosenfeld's sister. During the period of time in which Stephanie Rosenfeld's cellular phone was illegally wiretapped, Danielle and Stephanie engaged in dozens of communications that were intercepted and recorded. Danielle Rosenfeld did not consent to the interception or recording of any of these communications. Under the Wiretap Act, she is entitled to statutory damages in an amount of the greater of $10,000 or $100 for each day on which her

communications were illegally intercepted or recorded, as well as punitive damages in an amount to be determined.

9. Plaintiff Vincent Garcia is a citizen and resident of New York. He is the uncle of Det. Lemieux. During the period of time in which Det. Lemieux's cellular phone was illegally wiretapped, Mr. Garcia engaged in several communications with Det. Lemieux that were intercepted and recorded. Mr. Garcia did not consent to the interception or recording of any communications. He is entitled to statutory damages in an amount of the greater of $10,000 or $100 for each day on which his communications were illegally intercepted or recorded, as well as punitive damages in an amount to be determined.

10. Defendant Tara Lenich is a citizen of New York, currently imprisoned and residing in Connecticut at the Federal Corrections Institution in Danbury. At all relevant times, Ms. Lenich was the Deputy Chief of Special Investigations of Violent Criminal Enterprises at the KCDA, acting in the capacity of agent, servant, and employee of Defendant City of New York, within the scope of her employment as such, and under color of state law. Ms. Lenich was responsible for the policy, practice, and supervision of KCDA wiretap operations and oversaw KCDA wiretaps stemming from firearms, narcotics, vice, and gang investigations. Ms. Lenich is sued in her individual capacity.

11. Defendant Lu-Shawn M. Thompson is a citizen and resident of New York. She is the Administrator of the Estate of Kenneth P. Thompson, who is deceased. From 2014 until his death on October 9, 2016, Kenneth Thompson was the District Attorney for Kings County, acting in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and acting under color of state law. Mr. Thompson was responsible for the policy, practice, supervision, implementation and conduct of all KCDA matters and was

responsible for the training, supervision, and conduct of all KCDA personnel, including Ms. Lenich and the other individual defendants. Lu-Shawn Thompson, as Administrator of the Estate of Kenneth Thompson, is sued for the acts and omissions of Kenneth Thompson in his individual capacity.

12. Defendant Eric Gonzalez is a citizen and resident of New York. From 2014 until approximately October 9, 2016, Mr. Gonzalez was the Deputy District Attorney for the KCDA; from October 9, 2016, until approximately January 21, 2018, Mr. Gonzalez was the Acting District Attorney for Kings County; since January 21, 2018, Mr. Gonzalez has been the District Attorney for Kings County. In all three roles, Mr. Gonzalez acted in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and acting under color of state law. Mr. Gonzalez was responsible for the policy, practice, supervision, implementation, and conduct of all KCDA matters and was responsible for the training, supervision, and conduct of all KCDA personnel, including Ms. Lenich and the other individual defendants. Mr. Gonzalez is sued in his individual capacity.

13. Defendant William Schaeffer is a citizen and resident of New York. At all relevant times, Mr. Schaeffer was an Executive Bureau Chief within the KCDA, acting in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and acting under color of state law. Mr. Schaeffer was responsible for the policy, practice, supervision, implementation, and conduct of KCDA matters and was responsible for the training, supervision, and conduct of KCDA personnel, including Ms. Lenich. Mr. Schaeffer is sued in his individual capacity.

14. Defendant Mark Feldman is a citizen and resident of New York. At all relevant times, Mr. Feldman was on the executive team for the KCDA's office, either acting as Chief

Assistant District Attorney or in his current role as Executive Assistant District Attorney for Crime Strategies. In those roles, he acted in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and under color of state law. Feldman is sued in his individual capacity

15. Defendant Brian Donohue is a citizen and resident of New York. At all relevant times, Mr. Donohue was an Assistant Deputy Chief Investigator within the KCDA, acting in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and acting under color of state law. Mr. Donohue was responsible for reviewing all judicial orders authorizing the KCDA to conduct wiretaps to ensure they were authentic and for the day-to-day oversight of KCDA's wire rooms. Mr. Donohue was also responsible for physically setting up the wiretaps in a designated, controlled location. Mr. Donohue was also a designated "system administrator" with access to the ADACS Title III Systems server, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. Mr. Donohue is sued in his individual capacity.

16. Defendant William Power is a citizen and resident of New York. At all relevant times, Mr. Power was KCDA's Chief Information Officer, acting in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and acting under color of state law. Mr. Power was a designated "system administrator" with access to the ADACS Title III Systems server, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. Mr. Power is sued in his individual capacity.

17. Defendant Michael Dowling is a citizen and resident of New York. At all relevant times, Mr. Dowling was a Detective Investigator in the KCDA, acting in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and

acting under color of state law. Mr. Dowling was a designated "system administrator" with access to the ADACS Title III Systems server, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. Mr. Dowling is sued in his individual capacity.

18. Defendant Joseph Piraino is a citizen and resident of New York. At all relevant times, Mr. Piraino was a Chief Investigator in the KCDA, acting in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and acting under color of state law. Mr. Piraino was a designated "system administrator" with access to the ADACS Title III Systems server, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. Mr. Piraino is sued in his individual capacity.

19. Defendant Robert Kenavan is a citizen and resident of New York. At all relevant times, Mr. Kenavan was a Detective Investigator in the KCDA acting in the capacity of agent, servant, and employee of Defendant City, within the scope of his employment as such, and acting under color of state law. Mr. Kenavan was a designated "system administrator" with access to the ADACS Title III Systems server, which stored the oral and wire communications that were intercepted during the illegal wiretap operation. Mr. Kenavan is sued in his individual capacity.

20. Defendant City of New York (the City) is a municipal corporation that is responsible for the disciplinary, management, and administrative practices of the KCDA. The KCDA, through its senior officials, promulgates and implements administrative policies, including those with respect to applications for wiretaps and the operation of wiretaps. The City is sued directly under 18 U.S.C. § 2520 and as principal for the acts of its employees, including Lenich, within the scope of their employment.

21. Defendants Thompson, Gonzalez, Schaeffer, and Feldman are collectively referred to as the "Supervisory Defendants."

22. The Supervisory Defendants, along with Donohue, Power, Dowling, Piraino, and Kenavan, are collectively referred to as the "Individual Defendants."

JURISDICTION AND VENUE

23. This Court has jurisdiction over this case pursuant to 28 U.S.C. § 1331, because the action arises under 18 U.S.C. § 2510, *et seq*.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b), because the acts complained of occurred in the Eastern District of New York.

JURY DEMAND

25. Plaintiffs demand trial by jury.

CLASS ALLEGATIONS

26. Plaintiffs bring this action on behalf of themselves and all others similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 23.

27. The proposed Class is defined as follows: All persons whose wire, oral, or electronic communications with Stephanie Rosenfeld's personal cellular phone ("Cellular Telephone #1) and/or with Jarrett Lemieux's personal cellular phone ("Cellular Telephone #2) were intercepted.

28. Excluded from the Class are Stephanie Rosenfeld and Jarrett Lemieux, the Individual Defendants, and any person who makes a timely election to be excluded.

29. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

30. The members of the Class are so numerous that joinder is impractical. The Class consists of hundreds of members, whose precise identity can be ascertained only by examination of records and data exclusively possessed by Defendants.

31. Virtually all of the questions of law and fact in this action are common to the Class, including whether the Class members' wire, oral, or electronic communications were intercepted in violation of § 2511 of the Wiretap Act and whether they are entitled to statutory damages pursuant to § 2520 of the Wiretap Act. The common questions of law and fact predominate over any questions affecting only individual Class members.

32. The claims of the representative Plaintiffs are typical of the claims of the Class. The violations of law alleged by the named Plaintiffs stem from the same course of conduct by the Defendants—namely, undertaking or permitting an 18-month long illegal wiretapping operation, which intercepted the wire, oral, or electronic communications of the Class members without their knowledge or consent. Like all other Class members, Ms. Rosenfeld and Mr. Garcia were subjected to a significant, unjustified, and unlawful invasion of privacy when their personal, private communications were intercepted, recorded, and listened to and/or read. All class members are entitled to statutory damages under the Wiretap Act, 18 U.S.C. § 2520, which provides for liquidated damages in the amount of $100 for each day of violation or $10,000, whichever is greater.

33. The named Plaintiffs will fairly and adequately protect the interests of the Class. As explained above, the named Plaintiffs' claims are identical to the claims of all other Class members and they are entitled to the same statutory liquidated damages—either $10,000 or $100

for each day of violation—as all other Class members. They have a personal interest in the outcome of this action and have retained competent counsel who will zealously pursue relief on behalf of all members of the Class. The law firms of Emery Celli Brinckerhoff & Abady LLP and Wiggin and Dana, LLP, possess the requisite resources, experience, and expertise to prosecute this action on behalf of the Class. There is no known conflict among the members of the Class or between counsel for the Class and its members.

34. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The amount of damages that each individual Class member is entitled to is relatively small in comparison to the complexity of the litigation and, given the resources of the Defendants, no Class member could reasonably afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, the individual Class members would be left without redress for the violation of their privacy rights. Moreover, even if the individual Class members had the incentive and resources to pursue individual actions, the prosecution of hundreds of separate actions would be inefficient and wasteful of finite judicial resources. Individualized litigation would also create the potential for inconsistent or contradictory rulings, especially as the members of the Class reside in different judicial districts throughout the United States. A class action presents fewer management difficulties, allows claims to be heard which might otherwise go unheard due to the relative expense of bringing an individual lawsuit, and provides the benefits of adjudication, economies of scale, and comprehensive supervision by a single court.

COMMON FACTUAL ALLEGATIONS

Legal Framework

35. Congress enacted the Wiretap Act (commonly referred to as Title III) in response to the Supreme Court's recognition, in *Katz. v. United States*, 389 U.S. 347 (1967), that individuals have a constitutionally protected privacy interest in the content of their oral and wire communications. The Wiretap Act establishes the statutory framework that governs the surveillance of wire, oral, and electronic communications, including by law enforcement officers and agencies. Along with the Foreign Intelligence Surveillance Act, which is not at issue in this lawsuit, the Wiretap Act provides "the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f).

36. The Wiretap Act authorizes law enforcement officers to intercept wire, oral, or electronic communications in investigations of certain enumerated offenses with prior judicial approval. 18 U.S.C. §§ 2516, 2518. In order to obtain judicial approval, law enforcement officers must demonstrate that there is probable cause to believe that the individual targeted is committing one of several enumerated criminal offenses. 18 U.S.C. § 2518(3)(a).

37. The Wiretap Act provides precise procedures that law enforcement officers must follow in order to obtain an order authorizing or approving the interception of wire, oral, or electronic communications. Subject to narrow exceptions, each application for a wiretap order *must* include:

a. the identities of the investigative or law enforcement officer making the application and of the officer authorizing the application;

b. a full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that an order should be issued;

c. a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

d. a statement of the period of time for which the interception is required to be maintained, including a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; and

e. a full and complete statement of the facts concerning all previous applications made to any judge for authorization to intercept communications involving any of the same persons, facilities, or places specified in the application.

18 U.S.C. § 2518(1). New York's analogous wiretap statute contains similar requirements. N.Y. Crim. Pro. L. § 700.20.

38. A judge may enter an order authorizing or approving interception of wire, oral, or electronic communications under the Wiretap Act or New York's wiretap statute only if the judge determines that:

a. there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular enumerated offense;

b. there is probable cause for belief that particular communication concerning that offense will be obtained through such interception;

c. normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

d. there is probable cause for belief that the facilities from which, or the place where, the communications are to be intercepted are being used, or are about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by such person.

28 U.S.C. § 2518(3); N.Y. Crim. Pro. L. § 700.

39. A valid wiretap order many not authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, and in no event may a wiretap be authorized for longer than thirty days. 28 U.S.C. § 2518(5); N.Y. Crim. Pro. L. § 700.10. An application for an extension of a wiretap order must set forth the results thus far obtained from the interception in addition to the other required statements referenced above. 28 U.S.C. § 2518(3); N.Y. Crim. Pro. L. § 700.20.

40. The Wiretap Act requires district attorneys to keep detailed records on the use of wiretaps and to file annual reports with the Administrative Office of the United States Courts. By law, district attorneys must file reports in March of each year containing the following information with respect to each application for an order or extension made in the preceding calendar year:

a. the fact that an order or extension was applied for;

b. the kind of order or extension applied for;

c. the fact that the order or extension was granted as applied for, was modified, or was denied;

d. the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

e. the offense specified in the order or application, or extension of an order;

f. the identities of the applying investigative or law enforcement officer and agency making the application and of the person authorizing the application;

g. the nature of the facilities from which or the place where communications were to be intercepted;

h. a general description of the interceptions made under each order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted; (ii) the approximate nature and frequency of other communications intercepted; (iii) the approximate number of persons whose communications were intercepted; (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order; and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interception;

i. the number of arrests resulting from interceptions made under each order or extension, and the offenses for which arrests were made;

j. the number of trials resulting from such interceptions;

k. the number of motions to suppress made with respect to such interceptions, and the number granted or denied; and

l. the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions. 18 U.SC. § 2519(2).

18 U.S.C. § 2519(2). Under State law, "each district attorney" must submit the report required by federal law in January of each year. N.Y. Crim. Pro. L. § 700.60.

41. Notwithstanding this requirement of state and federal law, the Administrative Office Wiretap Reports for Calendar Years 2015 and 2016—the two years during which Lenich carried out the illegal wiretap operation—indicate that "[n]o prosecutor's report" was received from KCDA. The Administrative Office Wiretap Reports for the years immediately preceding and following Calendar Years 2015 and 2016 do contain information reported by KCDA.

42. The Administrative Office assembles the data reported annually by courts and prosecutors and publishes statistics on state and federal wiretaps. During Calendar Year 2016, there were 3,168 authorized wiretap orders reported. The average length of an authorized wiretap was 44 days. The average cost per order was $74,949. In Calendar Year 2015, there were 4,418 authorized wiretap orders reported. The average length of an authorized wiretap was 43 days and the average cost per order was $42,216.

43. Ms. Rosenfeld's personal cell phone was tapped for approximately 213 days in 2015. Mr. Lemieux's personal cell phone was tapped for approximately 484 days in 2015 and 2016. The total length of the illegal wiretap operation was approximately 545 days, from June 2015 to November 2016.

44. The Wiretap Act provides that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of" the Act, "may in a civil action recover from the person or entity, other than the United States, which engaged in that violation, such relief as may be appropriate." 18 U.S.C. § 2520(a). "Appropriate relief" under the Wiretap Act includes equitable or declaratory relief where appropriate; damages, including punitive damages in appropriate cases; and reasonable attorney's fees and other litigation costs reasonably incurred. *Id.* § 2520(b). In most civil actions under the Wiretap Act, "the court may assess as damages whichever is the greater of—(A) the sum of the actual damages suffered by

the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each violation or $10,000." *Id.* § 2520(c)(2).

Conducting a Wiretap at KCDA

45. At all relevant times, any KCDA Assistant District Attorney (ADA) seeking to conduct a wiretap was required to file a wiretap application with a court of competent jurisdiction, along with an affidavit demonstrating the requisite probable cause and need for a wiretap.

46. KCDA policy requires that a supervisor, such as Lenich, approve these wiretap applications.

47. As a matter of custom or policy, once an order authorizing a wiretap is properly signed by a court of competent jurisdiction, the order is given to Defendant Donohue, an Assistant Deputy Chief Investigator, who is responsible for ensuring that the order is authentic and properly signed. As part of this review, Donohue was supposed to look for a raised judicial seal which, while not required, is standard on valid orders as a means of showing their authenticity.

48. Only those individuals named in an order authorizing a wiretap are permitted to review the communications that are intercepted through the wiretap. A wiretap order typically authorizes a minimum of two ADAs, as well as all of the supervisors above those ADAs in the chain of command, to review the intercepted communications. A wiretap order also typically authorizes identified law enforcement personnel who have been specifically trained on the parameters and requirements of the governing order to monitor and minimize intercepted communications.

49. In addition to authorized ADAs, five system administrators—Defendants Donohue, Power, Dowling, Piraino, and Kenavan—have continued access to the KCDA wiretap servers.

50. Before Lenich was promoted to Deputy Chief of Special Investigations of Violent Criminal Enterprises, KCDA wiretap operations were generally facilitated by the New York Police Department's Tactical Action Response Unit out of a clandestine NYPD location in Queens. In or around 2013, Lenich caused Defendant Thompson to invest funds to create separate "wire room" facilities, containing all necessary equipment, within the KCDA office at 350 Jay Street, so that she and other ADAs could conduct wiretap operations without having to involve members of the NYPD Tactical Action Response Unit.

51. Following the establishment of the KCDA wire room facilities, all KCDA wiretaps are required to be conducted using those facilities. KCDA policy did not permit wiretaps to be conducted using personal laptops. Nevertheless, it was widely known that ADAs, including Lenich, routinely accessed the server from laptops in unsecured locations.

The Illegal Wiretapping Operation

52. Lenich commenced her illegal wiretapping scheme in or around June 2015. She fraudulently replicated the signatures of various New York State Supreme Court Justices on documents that purported to be court orders. These forged orders purported to authorize the KCDA to intercept and record the oral and electronic communications transmitted to and from Cellular Telephone 1, a certain cellular telephone line belonging to Stephanie Rosenfeld.

53. Lenich accomplished the forgery using a rudimentary "cut and paste" method. She physically cut a copy of each judge's signature from a legitimate document and taped the signature onto the fraudulent documents she had created.

54. Lenich then presented the fraudulent documents to Defendant Donohue, who reviewed and accepted them.

55. Though none of the forged orders Lenich showed to Donohue had original signatures or a raised judicial seal, Donohue nevertheless approved them and sent the forged orders (or caused them to be sent) to Ms. Rosenfeld's cellular telephone provider.

56. Each forged order submitted to Ms. Rosenfeld's cellular telephone provider purported to authorize the KCDA to intercept and record the oral and electronic communications transmitted to and from Cellular Telephone 1 for a period of 30 days.

57. At the end of each 30 day period, Lenich created a new forged order using the same rudimentary "cut and paste" method, and Defendant Donohue sent the new forged order (or caused it to be sent) to Ms. Rosenfeld's cellular telephone provider, purporting to authorize the continued interception and recording of the communications transmitted to and from Cellular Telephone 1 for an additional 30 days.

58. In total, Lenich and Donohue submitted seven forged judicial orders to Ms. Rosenfeld's cellular telephone provider, resulting in the continuous, round-the-clock, interception and recording of all electronic and oral communications to and from Cellular Telephone 1 for a period of seven months.

59. Between June 2015 and December 2015, scores of individuals who communicated with Ms. Rosenfeld, including Plaintiff Danielle Rosenfeld, had their electronic and oral communications intercepted and recorded without their consent, in violation of the Wiretap Act.

60. All communications that were intercepted from Cellular Telephone 1 were stored on KCDA servers and were accessible to Defendants Lenich, Donohue, Power, Dowling, Piraino, and Kenavan, as well as to others who were provided access to the wiretap servers.

61. Beginning in or around August 2015, while the illegal wiretap of Cellular Telephone 1 was ongoing, Lenich began creating another series of forged judicial orders purporting to authorize the KCDA to intercept and record the oral and electronic communications occurring over Cellular Telephone 2, a certain cellular telephone line belonging to Jarrett Lemieux.

62. Lenich forged the orders targeting Cellular Telephone 2 using the same rudimentary cut-and-paste method that she used for the orders targeting Cellular Telephone 1.

63. She then presented the forged orders to Defendant Donohue, who reviewed and accepted them notwithstanding their lack of original signatures or raised judicial seals.

64. Donohue then sent the forged orders (or caused them to be sent) to Det. Lemieux's cellular telephone provider, purporting to authorize the KCDA to intercept and record the oral and electronic communications occurring over Cellular Telephone 2 for a period of 30 days at a time.

65. In total, Lenich and Donohue submitted seventeen forged judicial orders to Det. Lemieux's cellular telephone provider, resulting in the continuous, round-the-clock, interception and recording of all electronic and oral communications to and from Cellular Telephone 2 for a period of approximately sixteen months.

66. Between August 2015 and November 28, 2016, when Lenich was arrested, hundreds of individuals who communicated with Det. Lemieux, including Plaintiff Garcia, had

their electronic and oral communications intercepted and recorded without their consent, in violation of the Wiretap Act.

67. All communications that were intercepted from Cellular Telephone 2 were stored on KCDA servers and were accessible to Defendants Lenich, Donohue, Power, Dowling, Piraino, and Kenavan, as well as to others who were provided access to the wiretap servers.

68. Lenich used and disclosed information gleaned from the illegal wiretap operation for the purpose of harassing Stephanie Rosenfeld and Jarrett Lemieux.

69. The illegal wiretap operation ended on or about November 28, 2016, when Lenich was arrested and charged with two counts of eavesdropping under N.Y. Penal Law § 250.05 and two counts of criminal possession of a forged instrument in the second degree under Penal Law § 170.25. Subsequently, a federal grand jury indicted Lenich on two counts of illegal interception of communications in violation of 18 U.S.C. §§ 2511(1)(a), 2511(4)(a) and 3551, *et seq*.

70. As a result of Lenich's arrest, various media outlets reported on her illegal wiretapping operation, beginning on November 28, 2016. That is the earliest date on which any Class Member could reasonably have been aware that he or she was the victim of the illegal wiretapping operation and therefore might have a cause of action against the City and the Individual Defendants.

71. On April 3, 2017, Lenich pleaded guilty to both counts in the federal indictment. On February 2, 2018, she was sentenced to one year and one day in prison for each of the two counts, to be served concurrently.

The City's Liability for the Illegal Wiretap Operation

72. The City is liable for Lenich's actions because she conducted the illegal wiretap operation within the scope of her employment by the City; because she was a final policymaker

with authority to establish municipal policy with respect to KCDA wiretap operations; and because her misconduct was directly enabled and facilitated by a municipal policy of deliberate indifference toward the operations of the wiretap room.

73. As the Deputy Chief of Special Investigations of Violent Criminal Enterprises and a supervisor of the wiretap room facilities, Lenich had broad authority to initiate and oversee wiretaps without supervision and she routinely conducted wiretap operations without oversight or supervision.

74. Lenich conducted the illegal wiretap operation principally during working hours, on KCDA premises, and using KCDA equipment and facilities. The costs of the wiretap operation were paid out of KCDA funds.

75. Lenich conducted the illegal wiretap operation at least in part for the benefit of KCDA. During most of the period of time that the illegal wiretap operation was ongoing, Lenich was working closely with Det. Lemieux on a major criminal investigation. At her sentencing following her guilty plea, she testified that part of her motivation in eavesdropping on Det. Lemieux's conversations was that she was "trying to protect" her work on that investigation, which was "the biggest case of [her] career."

76. Lenich's misconduct was reasonably foreseeable because she had a past history of abusing her authority within the KCDA and had virtually limitless authority to conduct wiretaps. In addition, it was widely known that Lenich was responsible for causing KCDA to establish its own wire room facilities, thereby bypassing the participation of the NYPD Tactical Action Response Unit.

77. The City is also liable for Lenich's misconduct because she was a final policymaker with final authority to establish municipal policy with respect to KCDA wiretap operations.

78. In her capacity as Deputy Chief of Special Investigations of Violent Criminal Enterprises, Lenich reported directly to Defendant Schaeffer, the Executive Bureau Chief. However, she had the authority to report and make requests directly to Defendants Thompson and Gonzalez, without going through others in the chain of command.

79. She demonstrated her authority over KCDA wiretapping operations by, among other things, causing KCDA to establish wire room facilities within its office in Brooklyn, bypassing the participation of the NYPD Tactical Action Response Unit.

80. As Deputy Chief of Special Investigations of Violent Criminal Enterprises, Lenich supervised ADAs and detectives who conducted investigations within the KCDA and who installed wiretaps, including Defendant Donohue. Lenich had primary control over wiretap operations stemming from narcotics, firearms, vice, and gang investigations, with final policymaking authority with regard to whether to seek a wiretap, how to set up a wiretap, and how to conduct a wiretap.

81. If Lenich were not a final policymaker, she would not have been able to establish and maintain an eighteen-month-long "confidential" wiretap operation without interference from other KCDA supervisors.

82. The City is also liable for Lenich's misconduct because it was enabled and facilitated by a municipal policy or custom of deliberate indifference to the operation of KCDA wiretaps.

83. The Supervisory Defendants, who were final policymakers for the City, acting within the scope of their employment as agents of the City, knew or should have known that Lenich was acting without oversight or supervision with respect to KCDA wiretaps.

84. All told, between June 2015 and November 28, 2016, Lenich forged twenty-four judicial orders. Not one of these twenty-four orders contained an original signature or raised seal. Nevertheless, Defendant Donohue approved and sent (or caused to be sent) each and every one of the forged orders to Ms. Rosenfeld's and Det. Lemieux's cellular telephone providers, purporting to authorize a continuous, round-the-clock wiretap operation of Cellular Telephone 1 and Cellular Telephone 2 for nearly a year and a half.

85. Though Lenich claimed, for approximately eighteen months, that she was conducting a "confidential" investigation, the Supervisory Defendants knew or should have known that no such investigation existed.

86. The Supervisory Defendants must have been aware of Lenich's illegal wiretap operation because they were required by state and federal law to keep detailed records on KCDA wiretap operations, including information on the length of interceptions and the number and duration of any extension; descriptions of the interceptions, and the number of arrests resulting from the interceptions. It is inconceivable that the Supervisory Defendants could have maintained this information without realizing that Lenich was conducting an unauthorized and illegal wiretap operation.

87. Despite the requirements of state and federal law, the Administrative Office Wiretap Reports for Calendar Years 2015 and 2016 indicate that "[n]o prosecutor's report" was submitted from KCDA for the two years during which the illegal wiretap operation transpired.

88. The Administrative Office Wiretap Reports do reflect data provided by KCDA in Calendar Years 2013 and 2014, before the illegal wiretapping operation commenced. In 2013, KCDA reported 6 installed wiretaps with an average of 2.3 extensions per wiretap and an average total duration of 85.7 days. In 2014, KCDA reported 61 installed wiretaps, with an average of 1.4 extensions per wiretap and an average total duration of 61.6 days.

89. Had Defendants Thompson and Gonzalez complied with their statutory reporting obligation in 2015 and 2016, the data reported to the Administrative Office of United States Courts would have included at least two installed wiretaps that were not reflected in the corresponding data concerning judicially authorized wiretaps for KCDA that is separately reported by state and federal courts. KCDA's data for 2015 and 2016 would also have reflected that one of these wiretaps (which took place entirely in Calendar Year 2015) was extended six times and lasted approximately 213 days and the other (which began in August 2015 and continued through November 2016) was extended sixteen times and lasted approximately 484 days. This data, if collected and reported, would have revealed a stark disparity from the data reported for Calendar Years 2013 and 2014.

90. Had Defendants Thompson and Gonzalez complied with their statutory reporting obligations in 2015 and 2016, their data would also have been wildly out of sync with data reported by neighboring counties:

a. In 2015, Queens County reported 201 installed wiretaps, with an average of 2.7 extensions per wiretap and an average duration of 100.6 days. In 2016, Queens County reported 79 installed wiretaps, with an average of 2.9 extensions per wiretap and an average total duration of 107.6 days.

b. In 2015, Bronx County reported 35 installed wiretaps, with an average of 1.3 extensions per wiretap and an average duration of 55.1 days. In 2016, Bronx County reported 13 installed wiretaps, with an average of 1.7 extensions per wiretap and an average duration of 63.6 days.

c. In 2015, New York County reported 68 installed wiretaps, with an average of 2.3 extensions per wiretap and an average total duration of 95.8 days. In 2016, New York County reported 14 installed wiretaps with an average of 2.7 extensions per wiretap and an average total duration of 91 days.

91. The fact that the Administrative Office Wiretap Reports for Calendar Years 2015 and 2016 reflect that no report was received from KCDA for the two years during which Lenich conducted the illegal wiretap operation is further evidence of the City's policy or custom of deliberate indifference to KCDA wiretap operations.

92. But for a municipal policy or custom of deliberate indifference to the operation of KCDA wiretaps, Defendants Thompson and Gonzalez would not have been permitted to withhold wiretap data from the Administrative Office of U.S. Courts that is required by state and federal law.

93. But for a municipal policy or custom of deliberate indifference to the operation of KCDA wiretaps, it is inconceivable that Lenich could have submitted twenty-four forged wiretap orders over the course of eighteen months, authorizing two wiretaps that continued for over 500 days, at considerable cost to the KCDA, without raising questions about the nature of her "confidential" investigation and the necessity of further surveillance.

94. Despite their actual and/or constructive knowledge that Lenich was conducting unlawful wiretaps for a period of approximately eighteen months, the City and the Supervisory

Defendants permitted, tolerated, and were deliberately indifferent to Lenich's conduct, allowing her to intercept and record hundreds, if not thousands, of private communications between and among the Class Members and Ms. Rosenfeld and/or Det. Lemieux.

The Individual Defendants Use and Disclose Plaintiffs' Private Communications

95. The Individual Defendants each had access to the KCDA servers on which Plaintiffs' unlawfully intercepted communications were stored.

96. Defendants Donohue, Power, Dowling, Piraino, and Kenavan were designated system administrators with continuous access to the KCDA wiretap servers, including recordings of communications intercepted by the illegal wiretaps.

97. After Lenich's misconduct came to light, Defendants Schaeffer, Feldman, and Gonzalez were directly involved in the KCDA investigation of the operation and therefore had access to the illegally intercepted communications.

98. Defendants Schaeffer, Feldman, Gonzalez, Donohue, Power, Dowling, Piraino, and Kenavan each received, used, reviewed, and/or disclosed copies of telephonic and electronic communications that were unlawfully intercepted from Cellular Telephone 1 and Cellular Telephone 2.

99. Defendants Schaeffer, Feldman, Gonzalez, Donohue, Power, Dowling, Piraino, and Kenavan knew Plaintiffs' communications had been unlawfully obtained at the time they received, used, reviewed, and/or disclosed them because they knew Lenich had forged court orders to wiretap Cellular Telephone 1 and Cellular Telephone 2.

100. Defendants Schaeffer, Feldman, Gonzalez, Donohue, Power, Dowling, Piraino, and Kenavan used Plaintiffs' private, unlawfully obtained communications and disclosed them to one another, as well as to others, without Plaintiffs' permission.

101. Neither Plaintiffs nor any party to the intercepted communications consented to anyone from the KCDA using or disclosing Plaintiffs' private communications.

102. Following Lenich's arrest on November 28, 2016, KCDA employees talked about the contents of the communications that had been unlawfully intercepted from Cellular Telephone 1 and Cellular Telephone 2—none of which should have been disclosed to anyone.

103. Characterizations of the contents of communications that were unlawfully intercepted from Cellular Telephone 1 and Cellular Telephone 2 were splattered across the media, even though the contents of those communications should never have been disclosed.

COUNT ONE

(Wiretap Act, 18 U.S.C. §§ 2510 *et seq*., Against Lenich)

104. Plaintiffs repeat and reallege the forgoing paragraphs as if they were fully set forth herein.

105. The contents of Plaintiffs' oral, wire, and electronic communications were intercepted, recorded, used, and/or disclosed by Lenich in a manner not authorized by law, in violation of 18 U.S.C. § 2511(1).

106. Lenich acted intentionally and maliciously in violating Plaintiffs' rights under the Wiretap Act.

107. As a direct and proximate result of the violation of Plaintiffs' rights under the Wiretap Act, Plaintiffs sustained injuries and are entitled to statutory damages as set forth in 18 U.S.C. § 2520(c) and punitive damages.

COUNT TWO

(Wiretap Act, 18 U.S.C. §§ 2510 *et seq*., Against Thompson, Gonzalez, Schaeffer, Feldman, Donohue, Power, Dowling, Piraino, and Kenavan)

108. Plaintiffs repeat and reallege the forgoing paragraphs as if they were fully set forth herein.

109. The Individual Defendants are persons who engaged in the violation of Plaintiffs' rights under the Wiretap Act by permitting and/or facilitating the illegal wiretap operation to continue despite knowing, or having reason to know, that it was unauthorized or illegal.

110. The Supervisory Defendants—Thompson, Gonzalez, Schaeffer, and Feldman—knew or should have known that the wiretaps on Cellular Phones 1 and 2 were unauthorized or illegal and yet the Supervisory Defendants facilitated the wiretaps and/or were deliberately indifferent to them in violation of the Wiretap Act.

111. Defendant Donohue directly facilitated the violation of Plaintiffs' rights under the Wiretap Act by setting up the illegal wiretaps despite knowing, or having reason to know, that they were unauthorized or illegal.

112. The Individual Defendants—Thompson, Gonzalez, Schaeffer, Feldman, Donohue, Power, Dowling, Piraino, and Kenavan—used, reviewed, and/or disclosed Plaintiffs' electronic and oral communications, despite knowing that they had been intercepted without Plaintiffs' permission and in a manner that was not authorized under law, in violation of 18 U.S.C. § 2511(1).

113. The Individual Defendants acted intentionally and were deliberately indifferent to Plaintiffs' rights under the Wiretap Act.

114. As a direct and proximate result of the violation of Plaintiffs' rights under the Wiretap Act, Plaintiffs sustained injuries and are entitled to statutory damages as set forth in 18 U.S.C. § 2520(c) and punitive damages.

COUNT THREE

(Wiretap Act, 18 U.S.C. §§ 2510 *et seq*., Against the City)

115. Plaintiffs repeat and reallege the foregoing paragraphs as if they were fully set forth herein.

116. Lenich intercepted and recorded Plaintiffs' oral, wire, and electronic communications while acting in the course of her employment for the City, on City time, and using City equipment, facilities, and funds.

117. The City violated Plaintiffs' rights under the Wiretap Act through the actions of its agents and employees, including Lenich and the Individual Defendants, and is responsible for the results of their misconduct under the doctrine of *respondeat superior*.

118. The City is further liable for Lenich's decision to unlawfully intercept Plaintiffs' communications through illegal wiretaps because Lenich used her final decision-making authority to carry out the operation. Lenich was a final policymaker with respect to KCDA wiretap operations generally and with respect to the illegal wiretap operation specifically. Lenich had final decision-making authority over whether and under what circumstances to conduct a wiretap of Cellular Telephones 1 and 2, as well as the operation of those wiretaps.

119. The City is further liable for the acts and omissions of the Individual Defendants, including Lenich, because Lenich's misconduct was directly enabled and facilitated by a municipal policy or custom of deliberate indifference toward the operation of KCDA wiretaps in general and to the illegal wiretap operation in particular.

120. The City, through KCDA and its agents, including the Individual Defendants, acting under the pretense and color of law, permitted, tolerated, and was deliberately indifferent to the operation of KCDA wiretaps, such that Lenich was able to conduct a months-long "confidential" wiretap operation without oversight. This longstanding custom or practice allowed wiretaps to proceed under the authority of a single person, without oversight or periodic checks to verify the validity of the wiretaps, without checking the continued need for the wiretaps after

each 30-day period, or confirming continued compliance with wiretap obligations, such as minimization.

121. This deliberate indifference to KCDA wiretap operations generally, and to Lenich's misconduct in particular, constituted a municipal policy, practice, or custom and caused the unlawful interception of Plaintiffs' private communications.

122. As a direct and proximate result of the misconduct and abuse of authority described above, Plaintiffs sustained injuries and are entitled to statutory damages as set forth in 18 U.S.C. § 2720(c).

WHEREFORE, Plaintiffs respectfully seek:

1. An order certifying this action as a class action pursuant to Federal Rule of Civil Procedure 23(b) for the Class described herein and naming Plaintiffs as the Class representatives;

2. Statutory damages against Defendants in an amount to be determined as set forth in 18 U.S.C. § 2720(c);

3. Punitive damages against the Individual Defendants in an amount to be determined at trial; and

4. An award of reasonable attorneys' fees, costs, and disbursements.

Dated: November 26, 2018
New York New York

EMERY CELLI BRINCKERHOFF & ABADY LLP

Richard D. Emery
Samuel Shapiro
600 Fifth Avenue, 10th Floor
New York, NY 10020
(212) 763-5000

Attorneys for Plaintiffs

WIGGIN & DANA LLP

James I. Glasser
Tadhg A.J. Dooley
437 Madison Avenue, 35th Floor
New York, NY 10022
(212) 490-1700

Attorneys for Plaintiffs